Innovating Democracy

Scytl Australia Pty. Ltd

submission to support the

Report on the iVote system

Conducted by Mr. Roger Wilkins AO

on behalf of the NSW Electoral Commission in response to the NSW Parliament's Joint Standing Committee on Electoral Matters report on the 2015 State election.

This submission is made on behalf of Scytl Australia Pty. Ltd.,
a wholly owned subsidiary of Scytl Secure Electronic Voting S.A.

[redacted]

Sam Campbell
Director, Scytl Australia Pty. Ltd.
30 / December / 2017 - *amended*

Scytl - Secure Electronic Voting

STRICTLY CONFIDENTIAL

Use only for evaluation purposes.

Scytl Australia Pty. Ltd. is a wholly owned subsidiary of Scytl Secure Electronic Voting, S. A.

This report contains the following sections:

1 Executive summary

The move towards internet voting advances relentlessly forward. Bodies responsible for the running of elections are presented with the obligation to support and implement legislation, whilst somehow being prepared for whatever change that may be just around the corner. Declining attendance and increasing expectations of the community for digitally connected services creates an environment where the question moves from “why not” to “when”.

The most common question received by an electoral official:
“Why can’t we vote online?”[1]

Scytl Australia Pty Ltd (Scytl), a wholly owned subsidiary of Scytl Secure Internet Voting S.A., is pleased to present this document to the inquiry by the NSW Electoral Commission (NSWEC) concerning its iVote internet and telephone voting system, which follows the NSW Government’s response to the NSW Parliament’s Joint Standing Committee on Electoral Matters report on the 2015 State election.

Scytl notes that the terms of reference for the inquiry are:

- Whether the security of the iVote system is appropriate and sufficient.
- Whether the transparency and provisions for auditing the iVote system are appropriate.
- Whether adequate opportunity for scrutineering of the iVote system is provided to candidates and political parties.
- What improvements to the iVote system would be appropriate before its use at the 2019 State General Election.

With the framing of the terms of reference being largely policy decisions (“… are the transparency provisions appropriate”), Scytl feels it inappropriate to answer those questions directly. Scytl is however in a position to inform the NSWEC about matters relating to electronic voting protocols (such as those used in iVote and similar systems), various security risks we see, and recommendations on technical matters.

The purpose of this document is to address some topics that have arisen over time regarding internet voting and more specifically iVote, including the iVote Core Voting System (iVoteCVS). The intention of providing this information to the inquiry is to convey an understanding of how security is implemented in a secure online voting solution, and the background and supporting information to the security protocols. Recommendations are made to enhance that security, considering ‘where we are now’ and what has been seen in iVote during the term of Scytl delivery.

[1] Ian Brightwell, NSW Electoral Commission CIO, Australia, 2015

BUT WHY CAN'T WE ALL VOTE ONLINE?

The person in the street wants the ability to vote online, to be free to minimise his or her time investment when actually casting the vote by minimising their travel – to just "vote from the couch". The person in the street trusts the government to protect the vote that they cast – and also to protect all those other votes cast by all those other voters – as each vote is unique, valuable, and a core of trust in our democratic system. But the person in the street does not know the security that goes into that system, nor should they need to. The person relies on the government to make the right choices, and implement the right systems.

Another group of people in the street have a background in Information Technology (IT) or IT security systems, and know how general IT systems work. Assumptions are made about IT systems (there is a 3-layer web delivered application model, and the database is where the precious data is, and if I can get to the database I can get away with anything can't I?). Some of those who are educated in other IT systems make negative comments about electronic voting systems – "can the system be trusted? I know how these things work so I understand how it could be done – surely it's not too hard?" These people, as a whole, make assumptions and do not necessarily seek to understand how a secure online voting solution works.

Then there is the secure online voting researcher. Variously funded by companies such as Scytl to solve the technical problems in order to design secure online voting systems; and those who, for their own reasons, seek to stop online voting systems being used.

Scytl sees that the reason we can't all vote online is a combination of legislation, prevailing political context, risk appetite from electoral commissions, and a healthy dose of fear, uncertainty and doubt.

STEREOTYPES

In the book "Public Opinion", the author Walter Lipmann coined a term 'Stereotypes' where stereotypes are a response to the pictures we have inside our heads. *He reveals how stereotypes affect public opinions and how these individual opinions "are crystallized into what is called Public Opinion" (p. 19)*[2]. In forming stereotypes, the importance of facts is missed. Secure online voting is an area where the prevalence of the stereotype, the picture in the minds of many in the community, is not based on fact.

It appears that to be successful secure online voting must overcome stereotypes that are in the minds of some in the public and political spheres, and the key to that is to communicate facts around the implementation of secure online voting. This should counteract some of the fear, uncertainty and doubt.

[2] http://www.fromthelabbench.com/from-the-lab-bench-science-blog/a-review-of-lippmanns-public-opinion

Removing the Stereotypes

At Scytl we have experience with a large number of people getting to know a secure voting system in detail – from new staff, to observers, to clients, to security auditors. What we have generally observed from these people is:

- Secure online voting systems are very different to any other system they have used
- They need to understand the security conceptually, before they understand the implementation
- It has taken them some time to 'get their head around' the implications of the security model

In this document Scytl intends to convey facts about secure online voting, to reduce the impact of any stereotypes. This will not change the mind of the community overnight, however it does point to a path in which the industry has some communication to do.

Other Stereotypes – the Golden Standard

Talking to online voting researchers who are against online voting generally brings up comparison to the manual paper ballot system such as we use in Australia – and so it should. What is often not recognised in these discussions is the human error rate in paper ballot handling and counting. Naming paper ballots as a 'Golden Standard' is an unrealistic bar against which to bring comparison. Comparison of error rates between the systems (paper, postal, online) can be used to strengthen the voting solution as a whole.

Technology and Recommendations

Scytl is of the view that the greater risks in elections aren't through the use of secure online voting systems, rather they are from the established, well known, and widely discussed risks – such as the misrepresentation of information regarding elections and political entities – via both social media and traditional media channels.

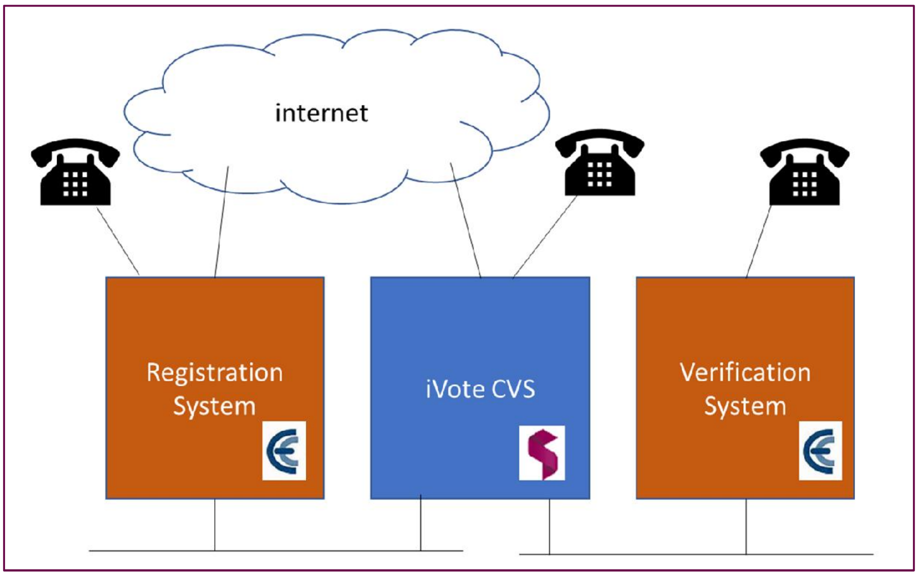
This document will provide technical coverage of the Scytl secure online voting protocol in an appendix for reference, and a higher-level description of elements of the protocol used in the iVote system in more of a layman's style in the body of this document. Some recommendations are provided; however these are limited to those technical areas where Scytl has implementation related expertise.

Please note that as this document is provided whilst the tender process is underway for the iVote update project, Scytl will hold over some recommendations, which will be included in the submission of its response to the tender process.

Scytl welcomes this inquiry, and will be available to respond to any further questions that may arise.

2 What is iVote and where does Scytl fit

iVote comprises three main components – the iVote Core Voting System (iVote CVS), the Registration System, and the Verification System. Scytl is the supplier of the software for the iVote CVS, as shown in the diagram below.



Following the tender by NSWEC for the development of the iVoteCVS in 2014, Scytl generated the iVoteCVS based on code from its Pnyx voting framework modified to suit the NSWEC requirement.

A full description of each of the systems is available from the NSWEC[3], but in summary:

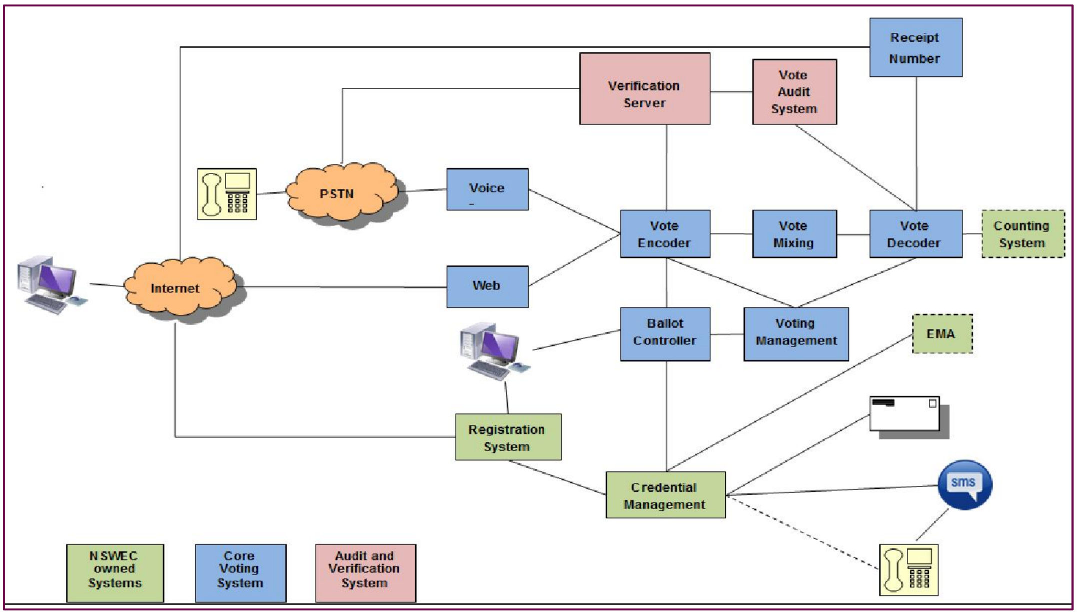
- The iVoteCVS:
  - Provides the voting interface the user sees
  - Provides an IVR interface for voting by phone
  - Responsible for the secure collection and storage of the vote
  - Separates the identity of the voter from the vote
- The Registration and Credential Management System:
  - Allows a voter to register to use the iVote system, either internet or call centre
  - Allows the facility to re-register
  - Provides the voting credential to the voter
- The Audit and Verification System:
  - Allows a voter to confirm over a phone that their vote preferences were recorded correctly

The iVote system is implemented and operated by the NSWEC, through various IT infrastructure service providers. The NSWEC can provide further information on this topic.

[3] http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/175758/iVote_System_Overview_v3.pdf

3 Secure online voting – what makes it secure

For reference, the NSWEC diagram of the iVote system is included here.

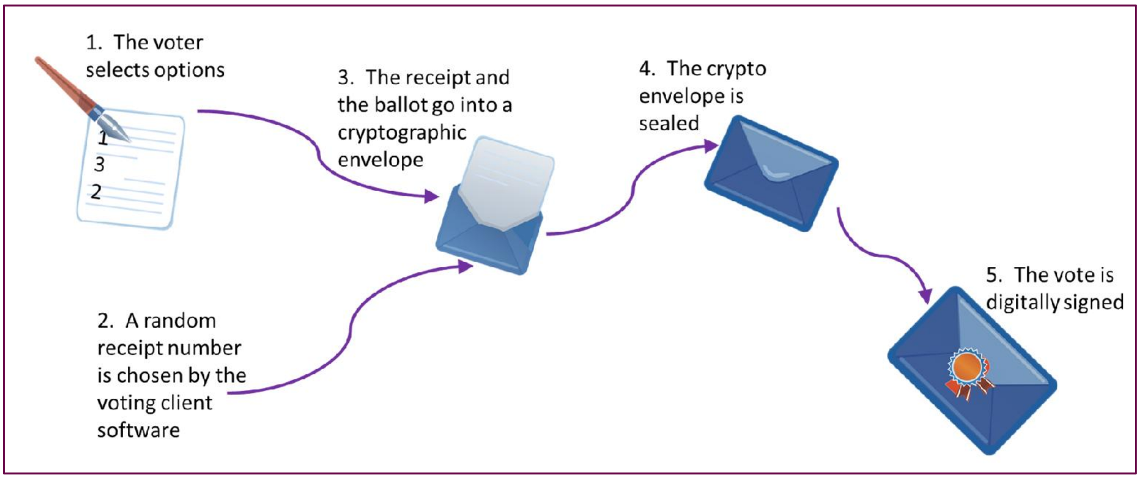


Many of the processes and elements of an online voting protocol have a heritage based on the regular paper voting process, and the postal voting process. As is shown in this section, many of the risks can be analysed in terms of the running of a postal ballot. The descriptions in this section are simplified a little for illustrative purposes, they do not describe all the security features or operational characteristics of iVote or other secure online voting systems.

This section is designed to challenge the stereotypes that people think of when reviewing an IT system, and specifically a secure online voting system.

3.1 How is a single ballot protected?

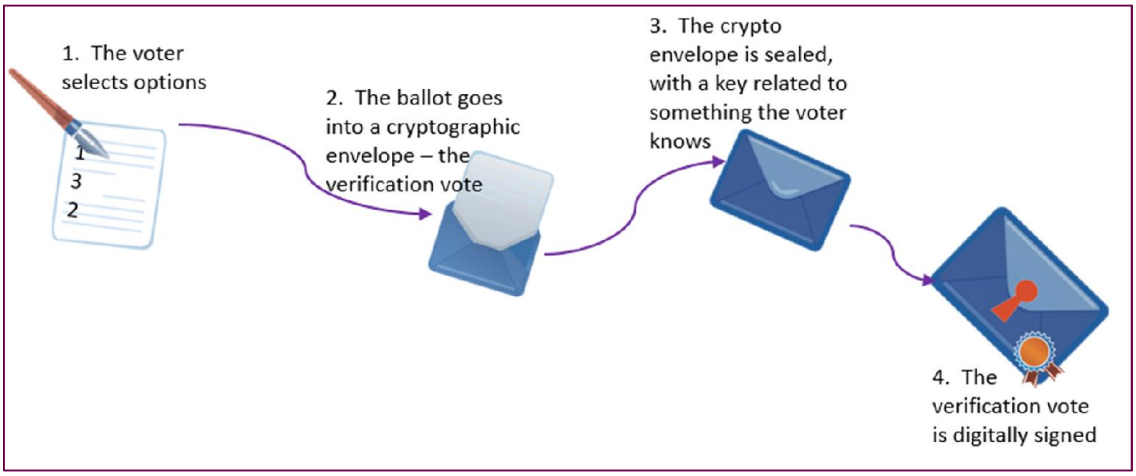
An electronic vote, in terms of the iVote CVS, is a populated electronic ballot paper which reflects the intentions of that voter.


1. The voter selects options
1
3
2
2. A random receipt number is chosen by the voting client software
3. The receipt and the ballot go into a cryptographic envelope
4. The crypto envelope is sealed
5. The vote is digitally signed

Key information about an electronic vote is:

- The electronic vote is encrypted to the public key of the election – forming the digital envelope
- A semi-random number is included inside the digital envelope (the receipt number)
- The digital envelope (containing the electronic vote and the receipt number) is signed by a private key allocated to the voter
- All this happens ***on the voters voting device***, transparently to the voter, through the Scytl JavaScript voting client
- The signed digital envelope holds a discrete secure electronic vote for that specific individual.

At the same time as the digital envelope is created, an alternate form of the vote is created for the Audit and Verification System.


1. The voter selects options
1
3
2
2. The ballot goes into a cryptographic envelope – the verification vote
3. The crypto envelope is sealed, with a key related to something the voter knows
4. The verification vote is digitally signed

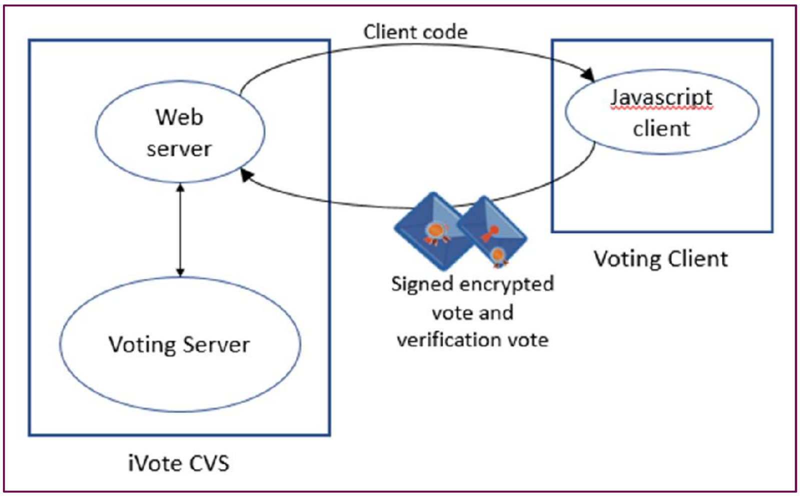
Key information about the verification vote is:

- The verification vote is encrypted into a digital envelope that has a key related to the voters PIN number
- The digital envelope (containing the electronic vote and the receipt number) is signed by a private key allocated to the voter
- All this happens ***on the voters voting device***, transparently to the voter, through the Scytl JavaScript voting client

Due to this combination of functions the following characteristics arise:

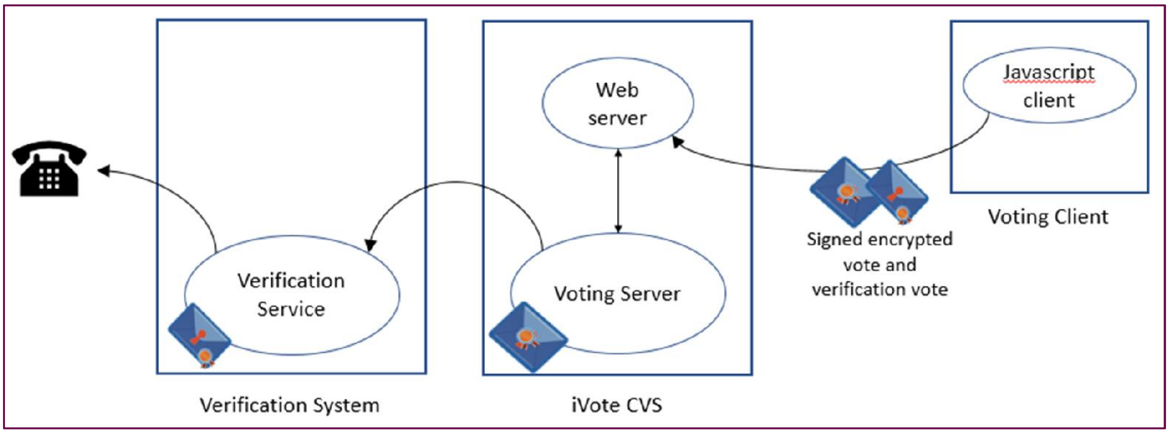
- The content of the electronic vote is protected by encryption, to prevent leakage of that voter's intention
- Any attempt to modify the vote will result in the signature on the secure electronic vote failing when it is tested, thus showing that this specific secure electronic vote has been tampered with and appropriate actions can be taken.
- These operations are all performed on the users voting device, ensuring that the electronic vote is secured prior to leaving the voters device.

- The electronic vote can be decrypted by the election private key
- The verification vote can be decrypted using something the voter who cast the vote knows.



3.2 The verification system

The Audit and Verification System allows a voter to contact the iVote service and listen to an audio replay of the content of their ballot. This allows them to report a discrepancy should they choose, and to cast another vote.



The verification system contains a copy of the ballot cast by the voter. As for the iVoteCVS, this ballot is encrypted and processed entirely on the users voting client.

3.3 The election private keys

When using asymmetric key cryptography, one of the keys is designated private, and the other public. The public key for the election is readily available through the iVote CVS as you would expect, however the private key is treated in an unusual way on the iVote system.

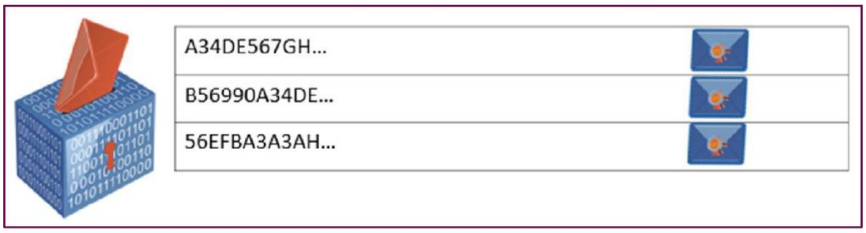
Scytl uses a process of splitting the private key into a number of parts at the start of the election.

The election key (private key) is split into N shares, with a quorum of P shares required to fully reconstruct the key. Each of these shares is placed on to a PIN-protected smartcard. N and P have been selected by NSWEC – what this means is that the election private key, which is the key that can be used to decrypt the votes in electronic envelopes, does not exist in usable form during the election. The holder of each smartcard only has access to his/her piece of the key.

Thus, during the election, all votes are encrypted from the time they are encrypted on the voter's device as described in section 3.1, until the key is reconstructed by a quorum of the key holders at the end of the election on an air-gapped machine.

3.4 Protecting the votes when in the server

The digital envelope containing each electronic vote is stored in a digital ballot box in the iVoteCVS. The digital ballot box is contained in an [redacted] database that communicates with the iVoteCVS, in effect each electronic vote is a row in the [redacted] database.



As each row in the database is a discrete electronic vote, this allows for the following features:

- There is a level of *measurable integrity* of the ballot box at a point in time.
- Should someone (an intruder or a trusted insider) gain access to the database server running the electronic ballot box, any alteration to one or all of the electronic votes is detectable.
- The specific tampered votes can be determined, as well as statistics such as how many and when.

This integrity check is performed daily, and at the end of the election, although it could be automated and configured to run regularly on the iVoteCVS and reported from the environment to an external monitoring service.

One tampered ballot does not bring the whole ballot box into question – that one ballot can be investigated to understand what has occurred.

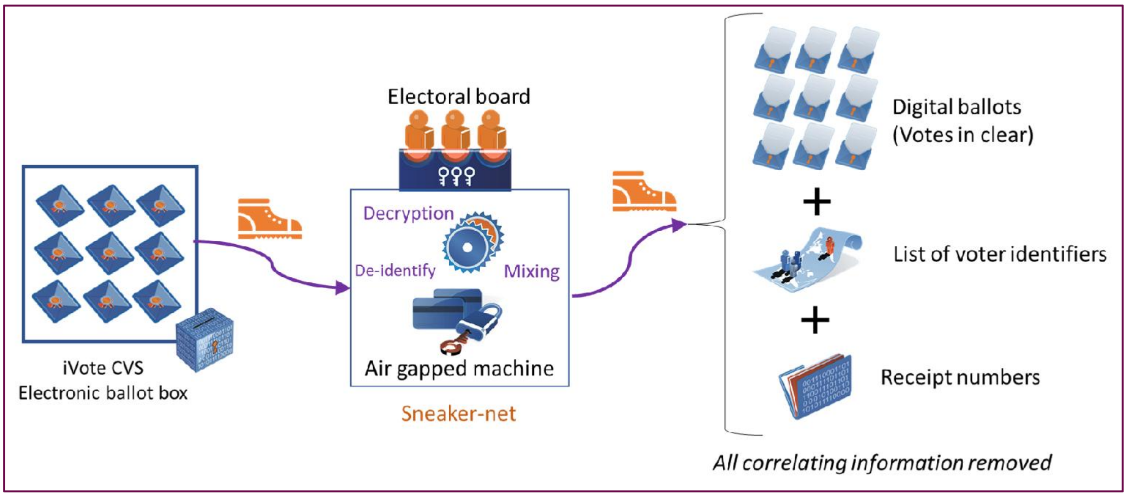
3.5 Decrypting the votes – preserving privacy

At the end of the voting process, the election is closed and the iVoteCVS stops receiving votes. The electronic ballot box is then transferred to an air-gapped (offline) machine where votes are decrypted and mixed using a mixing protocol – refer to the image below. The purpose of the mixing protocol is to ensure that the ballots are properly decrypted, without compromising the privacy of voters. To achieve this, the correlation between the voter and his/her electronic ballot is broken. A detailed description of this is described in Appendix A:

- **Ballot box integrity control:** Each ballot is checked for authenticity by validating that their electronic signatures are valid. Ballots that fail are reported and isolated.
- **Reconstruction of Election key:** The election private key is reconstructed from the smartcards that hold the shares. To proceed, a quorum of the key components is required.
- **Ballot mixing:** Valid electronic votes have their digital signatures detached. Then a shuffling process takes place to randomise the order of the votes in the system – this breaks any relationship to the voter based on the order of being read into computer memory and so forth.
- **Receipt number retrieval:** The random receipt number is retrieved from each electronic vote for publishing following the election.
- **Export of results:** The results are then exported from the offline machine, and can be included in the count by the NSWEC.

This mixing of the ballot box assists with preserving the privacy of the individual voter by separating the vote from the individual's identifier.

The receipt numbers are then published to a receipt number lookup tool on the NSWEC website at the close of the election – this provides the voter with the ability to lookup their receipt number and gain comfort that their vote was successfully decrypted.



3.6 Other checks and balances

Listed here are other points related to iVoteCVS and secure online voting systems, all or which support the security model that underpins the system.

3.6.1 Verifying the Verification System

Following the decryption ceremony at the end of an event using iVote, there is a further verification step, where the contents of the electronic ballot box and the verification system are compared and confirmed to hold equivalent content.

This step confirms that if one of the systems is compromised, this will be revealed through this comparison, providing an additional integrity check of each vote in the electronic ballot box.

3.6.2 Scytl Immutable Logs

Scytl has implemented the Scytl patented secure logging service, Scytl Immutable Logs, in the iVoteCVS. Scytl Immutable Logs implements cryptographic measures to preserve the integrity and authenticity of election logs. This logging technique is designed to preserve the log integrity at log entry level. Periodical checkpoint signatures are also generated to preserve the log authenticity and non-repudiation.

The main advantage of immutable logs, compared with digitally signed logs, is that they allow the location in the log trail of when a manipulation took place on the system. Manipulation of Scytl Immutable logs means that specific entries can be tested for their authenticity, whereas on a digitally signed log the whole log is invalidated when a corruption or invalidation occurs.

> Note: Scytl immutable logs work very much like a blockchain, only it is not distributed across a number of untrusted machines. It is however a chain of messages, signed to verify the origin and placed in a chain to present trust. Scytl has used this technology that was patented early in Scytl history, as it solves a number of problems around trust and auditability. Following extended research, Scytl is very careful with claims of 'voting on the blockchain', as this generally is based on a vote being stored on the blockchain. If a vote is stored on the blockchain, and the encryption cipher is cracked (as is known to happen over time) - what is the impact of all the votes being decrypted showing who voted when and for who?

3.6.3 Parallels with paper

The items described so far discuss the technical steps taken to protect the iVote system, however there is more done, and that is in the operational space. The following are examples of steps that occur which form additional components of the security context within which the iVoteCVS operates:

- Validation that the electronic ballot box is clear at the start of the election

- Specified roles for operators
- Shaking the ballot box prior to opening
- Enveloped ballots similar to postal voting

3.7 Bringing it together with traditional network security

The protective elements around Scytl secure electronic voting solutions, and specifically iVoteCVS have been described, and these show elements like the concept of the vote being protected before leaving the voters device, parallels with the paper process, the logging within the system, and the use of signatures to provide an ability to not only detect damage should it occur – but actually the amount of damage.

On top of the architecture outlined above is layered the standard IT network defences you would expect in a standard commercial system. This takes an already strong system, and applies the accepted principles of defence in depth to the solution.

Whilst network infrastructure questions should generally be directed to NSWEC, other elements utilised to strengthen the iVoteCVS include:

- Communications are protected by SSL
- Immutable logs are integrated with a monitoring system
- Operational healthchecks
- The system has all user accounts locked out during the execution of elections
- Digitally signed configuration files to ensure an acceptable configuration is in place

It is the fact that the iVote communications, like other products based on the Scytl Pnyx, are encrypted at the application layer that prevented Scytl products being affected by the Heartbleed attack in 2014. With the Heartbleed attack, by breaking through an SSL tunnel, attackers were able to snoop on data in memory, thus releasing protected information. As the Scytl voting server encrypts voting data in the client, and *it remains encrypted for its lifetime in the server*, the information was not able to be leaked from this vulnerability.

Finally, it is worth noting – the monitoring of iVoteCVS and other secure online voting solutions by Scytl is different to monitoring of most IT systems that people are familiar with. Many would consider it easier. Whilst the data stored in the electronic ballot box and travelling on the network is encrypted, *it has a uniform and predictable structure*. This makes the monitoring of the iVoteCVS environment easier, as all traffic that does not fit the predictable data profile becomes worthy of investigation.

What has been shown here are the steps taken to protect the secrecy and integrity of the vote, from each individual vote, to the collection of all votes in the ballot box. This is significantly different to other

IT systems in general use, a fact hidden from the general voter on the iVote system by way of its plain functional user interface.

4 iVote under attack – WA

In looking at recommendations relating to iVote, it is worth looking at the recent use of iVote in the recent Western Australian (WA) State General Election (SGE). As a result of the work by researchers into iVote for the WA-SGE, a number of claims were made[4]. These claims are reviewed here as they draw out the real-world applicability of some of the security features in the iVote system.

Claim 1: Anti-DDoS cloud providers have privileged access to voter credentials and ballots by virtue of their inherent man-in-the-middle (MitM) position between voters and the election website

- Encryption is not end-to-end between the voter and the election website. Data about the voter potentially exists at in an unencrypted form on the cloud provider's server
- To fingerprint clients as part of their anti-DDoS protection strategy, the cloud provider injects obfuscated JavaScript into the main page of the voting website in which a malicious man-in-the-middle could use to hide vote stealing malware.

SCYTL RESPONSE:

- The fact that a voter can verify their vote using the verification system mitigates a MitM attack that could manipulate the vote.
- Anti-DDoS cloud providers are specialist security providers who provide this service for multiple private and government services. They are considered trusted providers by the Government who selected them, and are therefore presumably equivalent to other government service providers.
- This is a similar issue to that faced by paper ballots through the post, in that the DDoS provider has trusted access much like the postal service.

Claim 2: The "double-encryption" mitigation of iVote in WA is not cryptographically secure.

- We built a test credential recovery tool that could recover a voter's PIN in about 1 minute for the cost of $1 worth of cloud computing
- A more detailed discussion of the double encryption login process was provided by the researchers.

SCYTL RESPONSE:

- The main problem is the need to support IVR friendly credentials. That means only numeric values: 8 numerical ID and 5 numerical PIN. So the strength of the authentication mechanism was only 60 bits. This was a design specification from the NSWEC.

[4] https://whisperlab.org/blog/2017/Trust-Implications-of-DDoS-Protection-in-Online-Elections.html

- Using the same length but with alphanumerical characters (as Scytl have used in Norway, Switzerland, France…) we can reach 80 bits entropy, something that made the attack difficult to implement in the short term. If we use 20 characters such as in Switzerland (XXXX XXXX XXXX XXXX XXXX) we reach the 112 bits of entropy recommended by standards.
- This is an attack easy to stop if we use alphanumerical credentials and the length of the credential is increased.

Claim 3: The highly multi-national nature of cloud providers exposes elections to state actors

- We did an internet wide scan on election day and confirmed the election website's public key certificate was serving out of Incapusla data centers around the world (including China).

SCYTL RESPONSE:

- This is only a problem for overseas voters, as national traffic does not leave Australian mainland as a general rule. If we simplify and assume that this affects China travellers, this is a comparable attack as that by the China postal service on postal votes.

Claim 4: We observed the cloud provider bundling numerous unrelated websites under a single public key certificate

SCYTL RESPONSE:

- Scytl understands that this is resolvable with the provider depending on the service offer selection by the customer.

Claim 5: We outline a scenario in which a national security agency of one country can make a lawful surveillance request on a domestic target, yet wind up with the private key used to identify the election server.

SCYTL RESPONSE:

- The same issue could happen with postal service. The difference is that postal votes are not encrypted and digitally signed, so easier to spy on and manipulate.
- Postal votes cannot be verified by the voters.

Despite the commentary above, Scytl has previously recommended against the use of this form of DDoS to our customers, as this form of attack is predictable and can be expected. Alternate DDoS solutions are available and should be used in future. DDoS solutions are outside the scope of the Scytl iVoteCVS solution. A recommendation is made to this effect.

A similar review of the attack against iVote in the 2015 election was undertaken by Scytl at the request of the NSW parliament. This document is available on the NSW parliamentary website[5].

[5] https://www.parliament.nsw.gov.au/committees/DBAssets/InquiryOther/Transcript/10263/Response%20to%20Questions%20on%20Notice%20by%20Mr%20Sam%20Campbell.PDF

5 International experience

Scytl includes here some observations based on international experience – Norway, a Scytl customer who stopped their trials, Belgium and their decision to forego the use of technology for elections, and Estonia and their use of a competitive solution to Scytl. These examples do not speak to the security of online voting systems, rather they reflect some stereotypes that apply in this field, the response in partisan vs bi-partisan environments, and comparison to the paper voting system.

NORWAY

Norway utilised a Scytl secure online voting solution for their 2011 and 2013 elections. This was a technically advanced system, utilising a different approach to voter verification than that utilised in iVote. Varying reports can be found regarding the demise of that project, however Scytl notes that the party who won the 2013 election did so with a view to '*stop this (electronic voting trial) and save the administration, bureaucracy, the Ministry of … and Taxpayers …*'[6]. From the debate referenced in the footnote, Michael Tetzschner was in opposition in Norway in 2010, and argued, along with others, to stop the funding of the electronic voting trial. This then came to pass when his party came to power as part of a coalition in 2013, the year of the last trial.

It is Scytl's view that this project appears to have been stopped for political reasons, rather than security reasons as has been claimed by some.

THE NETHERLANDS

Whilst not related directly to online voting, the Dutch example is one worthy of examination – a paper on the situation is available in the proceedings of the 2017 eVoteID conference[7] "The peculiar case of the Netherlands 2017" p315. The paper is used as a source for this section.

The preparations for the Dutch elections of 2017 took place in a "somewhat turbulent climate". This was in the context of following soon after the November 2016 US presidential elections. In the leadup to the elections "Various real and self-proclaimed 'experts' expressed their concerns. After a week, discussions had become so intense that a debate was scheduled in the Dutch Lower House." The stereotypes took over.

This lead to a decision being made by the Minister to *"… prohibit the use of all supporting software for the upcoming elections that were set to take place within a month."* The outcome, as described in the paper included errors in counting, errors in reporting, and official investigations being conducted.

The errors due to human error increased to significant levels. It could be argued on this basis that elections that have no automation that error rates are significant, and that the 'gold standard' of using

[6] https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2010-2011/101119/2/

[7] https://www.e-vote-id.org/wp-content/uploads/2017/10/TUTPress-2017.pdf - Peter Castenmiller and Kees Uijl

paper ballots and manual processes against which secure online voting is measured may be an unfair proposition.

A move towards additional channels for collecting votes, of which secure online voting is an obvious choice, leads to an electoral commission having information against which to balance the results of other channels. Is the voting trend on secure online voting different to attendance voting? Do we have suspect results in a particular area against which to detect errors in the paper system or the iVote system? These are questions the NSWEC is in a position to address as part of it's monitoring of an electoral event.

Estonia

Estonia is interesting to review also, for the reason that it has similarities to the Australian context when looked at through the prism of internet voting and the market response. A paper on the situation is available in the proceedings of the 2017 eVoteID conference[8] "Bits or Paper: which should get to carry your vote?" p156. The author makes the claim that paper voting is not inherently more secure than internet voting, and goes on to discuss. This paper appears to have been written by way of response to commentary by academic researchers in the online voting field directly targeting the project by the Estonian government.

In 2014 a team lead by Alex Halderman made a press release relating to the Estonian online voting system security just days prior to the running of an election[9]. The timing is reminiscent of the timing of tour and media events by Halderman and Teague in NSW during the NSW SGE in 2015.

It's worth noting that there are significant technical differences between the iVote system and the Estonian internet voting system, the key difference being that the Estonian system will not work in Australia due to its reliance on the Estonian national ID card.

In Estonia online voting appears to have bi-partisan support, based on the continuation of online voting since 2005 and through changes in Government. In the 2015 parliamentary elections 30.5% of participants voted over the internet[10]. Estonia has published some very interesting data related to online voting, where you can see for example an increase over time of older age voters using their system.

What we have observed at Scytl, is that the more successful a project is on a world scale, the higher the likelihood that recognisable negative internet voting researchers will turn out in opposition.

[8] https://www.e-vote-id.org/wp-content/uploads/2017/10/TUTPress-2017.pdf - Jan Willemson
[9] https://estoniaevoting.org/
[10] http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics

6 Other matters

6.1 Open source software

Scytl does not support the general view that open source software is the only solution for transparency in an electronic voting platform.

Over time Scytl has published in conferences cryptographic protocols to allow public review of its design and facilitated access to its source code to auditors selected by our Customers. Scytl sees no compelling reason to vary this position. In the past Scytl has released source code to the internet for specific customers.

- To open source a secure online voting solution opens the door to a potential avalanche of inquiry over matters related to code structure, design choice, personal preferences of programmers, taking away resource from where it is needed- to review the code to continue to improve it and ensure its security.
- An activist intent on disrupting an election could find a point of interest in the source code, regardless of its veracity, and use that as a toe-hold to destabilise an election by releasing it just prior to, or as an election starts. This would be similar to what was seen in the Netherlands in 2017 as discussed above.
- If an interested party finds a bug in the code that could be exploited, Scytl believes there is no guarantee that that information will be passed to the relevant commission, rather it will be knowledge with value to bad actors.
- Scytl secure online voting software is not a widely used system for which there is broad incentive for individuals to take on a systematic and thorough approach to code review, as is the case for apache software and other packages where these is broad interest in finding bugs and eliminating them.

Scytl prefers to allow voters the ability to verify their vote to gain confidence in the system rather than releasing source code. This view seems to be gaining popularity in the field. Anti-internet voting groups generally push for open source solutions, however Scytl has seen no evidence that this creates a more secure solution. Scytl is interested in working with the NSWEC to address issues related to transparency.

6.2 Postal system in decline

Australia Post has stated that use of the postal service is in decline, and it seems highly likely that the trimming back of postal services will be a regular occurrence due to unsustainable costs. There appears to be no viable alternative to postal voting for a number of voters if secure online voting is removed from the mix of alternatives to attendance at a polling booth.

What will happen if postal voting is no longer capable of returning votes within the allowed timeframes – will those voters become dis-enfranchised? This is a very real question to face electoral commissions in Australia and across the world.

Scytl sees that addressing issues with secure online voting is the best way for electoral commissions to meet the requirement for remote voting in the future.

6.3 Extending use from State General Elections

The cost of collecting hard to get votes is a challenge for electoral bodies, and in NSW that has been the basis for who is able to use the iVote system. Increasing the security of the iVote system can reasonably be expected to have associated costs, just as the iVote system appears to be financially viable from a cost per vote standpoint.

Increasing the costs associated with the running of iVote risk making the system less financially attractive to the electoral commission, whilst at the same time entering a time of potentially increased reliance on the system from a vote collection standpoint, associated with the decline of the postal vote.

In order to address these concerns, whilst not significantly increasing the risk profile of the iVote system, the NSWEC could:

- Utilise an enhanced version of iVote which includes a process for ‘iVote by attendance’, offered in Embassies and large vote collection centres. This version could offer paper verification slips allowing the voter to see in person that their vote is recorded as intended. This process would reasonably be expected to allay many of the issues raised by internet voting experts
- Utilise the iVote system for Local General Elections (LGE’s). As LGE’s are largely delivered using the postal system, the security model for the election is already significantly different to an SGE, lending itself towards an iVote solution.

Each of these variations would increase the cost, but also make a larger number of voters able to use the iVote system in a manner that would be seen as more secure. A reduced cost per vote when applied over an electoral term with these in place is easy to determine for the electoral commission.

6.4 Internet voting experts

Experts in secure online voting come from 3 main camps: the solution providers (Scytl included), the independent researchers with a keen and informed interest, and those who present themselves as independent researchers but for whom the answer is always ‘stop the project’ or something similar - activists.

There are many good ideas out there for enhancing electronic voting, and the base for many of them boils down to – investment. Invest in your people, invest in your process, invest in the right technology.

Use experts. Common threads you will see in any new technology. You will see these ideas pushed by companies like Scytl and its competition, and contained within submissions by researchers with a keen interest.

Internet voting seems to have attracted it's share of activists, and these activists are pushing the stereotypes so easily grasped by the public. Fear, uncertainty and doubt built on the what-if. The activists in electronic voting have some common traits – a background in science and IT, and in most cases little to no experience in the realities of running a broad-based government delivery project such as an election and all the logistics that that involves. There is a general approach of describing a scenario which is easily understood, but not necessarily realistic, and extrapolating that to say a project should be stopped because 'what-if'.

What separates the electoral commissions from these groups is the real-world experience of running an on the ground election, of understanding the risks associated with collecting a vote, and of understanding the impact of disenfranchisement in the community.

6.5 Verification – updating in iVote

The iVote solution relies on the ability for a voter to dial in and have their vote dictated to them by the verification service. A number of observers have attacked this verification system on the grounds it is opens the door to coercion. The implementation of this verification system is a specification by NSWEC in 2014. NSWEC noted when specifying the method of verification currently in use that coercion is not an issue in NSW (based on research from the University of NSW), and further that they wanted a system that could be easily explained in a court of law in case the system came under legal attack.

Alternate verification services are available, by Scytl and its competitors. Significant research and development continues in this space, as verification in the Australian context is not a simple problem to solve. A lower house ticket is not too challenging, however a full verification solution for a below the line vote in the upper house of NSW, with a minimal attack surface area from a security perspective is a problem with which researchers continue to struggle. Reports of usability of some solutions are now coming from the field that speak to user confusion, or user lack of confidence due to the opaqueness of solutions. This is not that the solutions are opaque, rather that they are transparent but not clearly understood by the uneducated person.

Is a different form of verification the next area activists will push for, then indicate that the solution is too complicated, then say 'stop the project'? This remains to be seen.

7 Recommendations

Scytl makes the following recommendations regarding the iVote system.

Rec 1: Reduce the functionality of the iVote demo system. The demo system should contain a version of the client that allows a voter to test the system for usability and that it works on their device. The current version contains a full implementation of the iVote voting client and thus opens the system up to reconnaissance. It is beneficial in system monitoring to see who is 'rattling the doorknobs' in order to detect an attack. With the long-term availability of the client on the demo system, reconnaissance can be performed months in advance of an actual attack.

Rec 2: Enhance monitoring of the electronic ballot box to be performed 'with a key press' and also to run at predefined intervals reporting success or failure.

Rec 3: Restrict the ability of the IVR based vote casting system (telephone voting system) to have a maximum number of votes per hour (for example). This prevents the IVR based vote casting system to become a significant attack vector, based on its short PIN number capabilities.

Rec 4: Modify the iVote system to require users to have longer credentials than currently in place. Alphanumeric PINs will increase the password space.

Rec 5: Modify the registration system to allow different authentication credentials for users who choose to use the IVR rather than internet voting.

Rec 6: Strengthen the iVote team in NSWEC on an ongoing basis. (Note – this appears to have happened already!)

Rec 7: Allow sufficient time for implementing projects. Scytl experience, after a number of projects in Australia and abroad, is that significant time is spent in the purchase phase, leaving little time for build and test. There is no 'one size fits all' approach in secure online voting due to local legislative requirements and so on. Time during implementation allows appropriate time for risk analysis and review.

Rec 8: Review alternate solutions for DDoS protection than that used for the WA election.

Rec 9: Foster interested persons in political parties to become involved in overseeing iVote, who can be drawn on to be scrutineers.

Rec 10: Implement 'iVote by Attendance', a system that has been discussed between Scytl and NSWEC in the past.

Rec 11: Remove the requirement to print paper ballots during a by-election, and use the process that is applied for the SGE.

Rec 12: Automate the lockdown / removal of lockdown procedures on the iVote system.

Rec 13: Remove command line operation where possible from iVoteCVS and other components to reduce the likelihood of user error.

A number of the recommendations are simple and can be implemented with patches rather than wholesale system redesign.

8 Conclusion

Scytl welcome this inquiry. Governments implement systems on an ongoing basis, and all too often issues arise which reach the newspaper headlines. Scytl views this inquiry as a checkpoint by the NSW Parliament into whether appropriate security can be implemented in iVote, and are the risks associated with that implementation worth it.

The iVote system has made headlines for two adverse security events - each of these actually against peripheral systems rather than the iVoteCVS or the ballot box. Whilst these attacks were against peripheral systems, Scytl acknowledges that the brand of "iVote" has been impacted, and this has drawn attention to secure online voting in NSW. Scytl sees that there is a role to play for Government, and for industry, to build confidence in this brand and this industry.

The WA and NSW issues are related to two recurring themes in government projects - budget and timing. Short time frame projects lead to compressed and pressured decision making - and not always for the best. These are situations with which Scytl is familiar as they are reflective of the electoral environment in other regions.

Why is iVote here? In Australia we have a compulsory voting system, and iVote fulfils the requirement of making voting easier for those who have challenges with the existing voting system – the blind, those who cannot move with ease due to disability, those who are travelling. Anecdotally Scytl believes that iVote holds the interest of electoral commissions across Australia, as it has the potential to help them to do their jobs – to fulfil the franchise. It's important to remember that the man in the street sees a need for online voting, and part of the education process is that online voting is not for all voters in all circumstances. *To maintain participation rates of 93%, the Electoral Commission cannot 'do nothing' given the decline of the Postal service.*

Scytl is of the view that the security of the iVote system is appropriate, however it is not sufficient today. The world has moved since 2014 when iVote was specified making the risk of guessing a credential higher than at that time. The inclusion of patches as described in the recommendations may make it sufficient – however this is a question for the state to answer. In order to fully answer the question, NSWEC must indicate their preferred method of verification and other technical characteristics that it believes will make the system security appropriate and sufficient. Scytl acknowledges that this is in part addressed by the current open tender process for the replacement of the iVoteCVS.

It is time to compare secure online voting systems as described in this document, with paper votes, postal votes, and the realities of regular elections. It is possible to identify that ballots are lost, it is possible to identify which votes have been tampered with, and investigations can be performed.

In conclusion Scytl believes that there are modest improvements to be made at this stage to the iVote system, taking into account the time until the next election, and known security issues that are currently in the iVote system. These can be addressed through patches as opposed to full system replacement.

Appendix A: Voting protocol detail – Pnyx

Please refer to the attached document “Scytl - Pnyx Whitepaper - voting protocol detail – attachment”. This document provides a detailed description of the Pnyx e-voting framework. This framework underpins much of the work Scytl has done to implement the iVote protocol. This attachment is provided for the reader to refer to, to gain further information than provided in the body of this document.

As this is the basis of the iVote implementation, specific detail regarding SSL parameters, cryptographic protocols and so on can be found in the NSW specification documents.

A.1 Attachment Abstract

Adequate cryptographic solutions are needed whenever an election is conducted by electronic means (poll-site electronic voting systems using digital ballots or networked voting systems with remote ballot casting). Scytl has developed a cryptographic e-voting framework to enable reliable and trustful electronic elections. Scytl’s e-voting framework ensures the authenticity of ballots, privacy of voters, accuracy of election results, secrecy of intermediate results, verifiability of election results by voters, and coercion resistance (the prevention of vote-selling and coercion of voters).

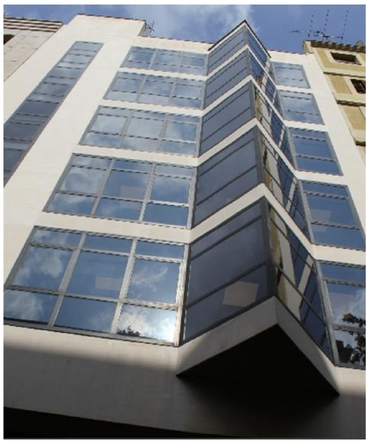
The document describes Pnyx.core, the software product developed by Scytl to implement the patented cryptographic protocols comprising Scytl’s e-voting framework. The most important among these protocols are: *the ballot casting protocol*, performed by voters in collaboration with a ballot box server; *the mixing protocol*, performed by electoral authorities to open the digital ballot boxes; and the *verification protocol*, that allows voters to verify their ballots against the published results ensuring that their votes have been correctly accounted for. Scytl’s e-voting product Pnyx.core, named after the hill in ancient Athens where elections were performed, forms the core of all Scytl’s e-voting solutions, and can be easily integrated into other electronic voting systems.

A.2 Attachment Intended Audience

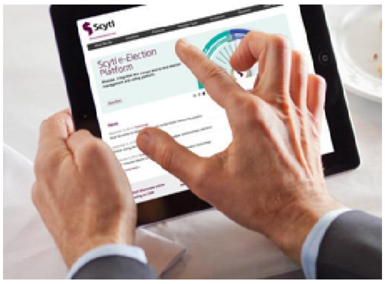
The intended audience of the document includes IT officers, security officers, managers, and other parties and individuals involved in the security of electronic electoral processes. The document is also interesting to parties evaluating and/or developing a transition process from traditional voting to any kind of electronic voting system (poll-site voting or remote voting), and who need to understand the benefits of using cryptographic e-voting frameworks.

Appendix B: About Scytl

B.1 Foundation and operation



Scytl is the global leader in secure election management, electronic voting and eGovernance solutions. Specialising in election modernisation technologies, Scytl offers the first end-to-end election management and voting platform, providing the highest security and transparency standards currently available. Scytl has capitalised on over 20 years of pioneering research to develop unique election-specific cryptographic security technology protected by the largest patent portfolio of the industry. Over these years, Scytl has accrued significant experience working with election officials in real elections.



Scytl's products have been successfully used in hundreds of projects worldwide, some of which represent breakthrough projects for the electoral modernization industry. Our solutions have been successfully used in over 40 countries across the globe: in Australia, New Zealand, Canada, the United States, the United Kingdom, France, Norway, Switzerland, Bosnia-Herzegovina, Brazil, the UAE, India, and Iceland. Scytl is headquartered in Barcelona, Spain, with strategic offices in Australia, the United States, Canada, Brazil, and Greece as well as field offices in the UK, France, Mexico, and India to name a few.

Scytl is based on strong scientific and research background. Formed in 2001 as a spin-off from a leading research group at the Autonomous University of Barcelona (Spain), the company has developed a strong track record of scientific achievements and recognitions. In fact, Scytl's founding research group has pioneered the research on electronic voting security in Europe since 1994 and has produced significant scientific results, including over 40 scientific papers published in international journals.

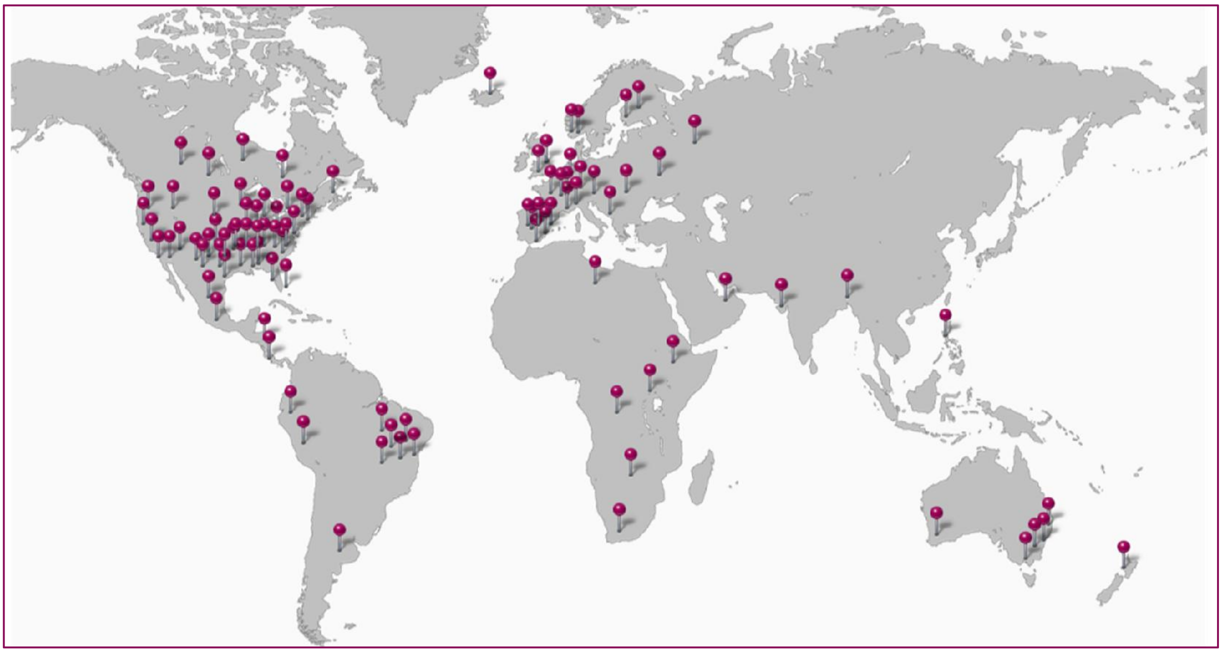
Scytl's ground-breaking cryptographic protocols provide elections with the highest levels of security, transparency and verifiability. Based on this core security technology, Scytl has developed an integrated set of solutions that addresses all the needs of both the Election cycle (before, during and after the elections) and the Governance cycle in between. In addition, and in compliance with international e-inclusion requirements, Scytl's products and solutions address the specific needs of disabled citizens, providing them the possibility to partake in elections without any assistance, while providing their privacy and allowing them to participate in the democratic process on equal terms.

With our strong scientific base, innovative research activities and unmatched worldwide experience, Scytl is the trusted electoral modernisation partner for demanding clients from both the public and private sectors. Public sector clients from local, regional (Municipal, State, etc.), and federal governments are leveraging Scytl's solutions to modernise their electoral and governance processes. Private-sector clients such as Universities and large associations are benefiting from Scytl's solution to carry out electoral/consultation processes such as labor union elections or shareholders' meetings.

Scytl consists of a global team of experienced professionals dedicated to the election modernisation industry who have worked with some of the largest electoral organizations. The experience gained managing over 1,700 election technology implementations, and over 100,000 electoral events, in over 40 countries has led to the development of tested and true methodologies, and a network of trusted partners that address the unique challenges faced by each client and their specific electoral requirements.

B.2 Scytl around the world

Scytl's clients span the world, with indicative references based in Australia, Switzerland, United States, Norway, India, France, Mexico, United Arab Emirates, Austria, Spain, Finland, United Kingdom, Philippines, Argentina, and so on. The map below shows an overview of where Scytl has delivered electoral modernisation projects.



Scytl projects (map)

B.3 Awards

Scytl has received numerous international and national awards as recognition of its ground-breaking work in electoral modernization and electronic voting. These distinctions were awarded to Scytl's technology and projects, as well as the company itself. The list below shows a selection of some of the many prestigious awards that Scytl has received.

- 2015 Innovative Practices award, Zero Project, for the work done in Victoria Australia.
- 2015 European Tech Tour Special Jury Award, European Tech Tour Association
- European Business Awards National Champion 2015 & 2014, RSM International
- Frost & Sullivan, 2014 Government Online Voting and Election Modernization Innovation and Leadership
- Best Performing BPO Ecuador 2013 Elections, I.R.I.S
- Longhorns Bully Award Champions of European Innovation, White Bull
- IST Prize by the European Commission to best technology (Pnyx e-Voting)
- Finalist and Best-Case Award for Madrid Participa by the European Commission
- European Venture Contest award for best technology company in Europe
- Leaders of the ITech-economy issued by the IE-Club Paris
- Winners by White Bull for the top technology and media leaders, entrepreneurs, innovators, investors, and visionaries and many more…

B.4 Audits and Certifications

Scytl's innovative, secure and transparent solutions have been audited and certified against extremely demanding, and highly strict system and security standards by prestigious certification authorities, universities and subject matter experts in multiple countries, including USA, UK, Australia, France, Finland, Switzerland, Austria and India. Scytl is the company with the highest number of certifications and audits in the field of electronic voting, for which certifications and audits are typically very thorough. The list below indicates some of the organizations that have audited Scytl's technologies:

- European Commission (EU)
- Federal Chancellery (Switzerland)
- City of Barcelona (Spain)
- Electoral Commission (Philippines)
- State of Victoria (Australia)
- State of Gujarat (India)
- State of Florida (US)
- Federal Voting Assistance Program (US)
- Ministry of Science and Research (Austria)
- Ministry of Justice (UK)

- Ministry of Local Government (Norway)
- Ministry of Foreign Affairs (France)
- Electoral Commission (UAE)
- Instituto Electoral Distrito Federal (Mexico).

B.5 International e-Voting Advisor

With its extensive experience and large knowledge capital, Scytl has been an advisor to numerous governments, institutions and election organizations worldwide including, but not limited to, the USA Federal Electoral Assistance Commission, the National Institute of Standards and Technology (NIST), the Council of Europe, several regional governments in Spain and the Austrian Ministry of Research and Science.

For example, the Organization of American States selected Scytl to audit the e-voting software developed by the National Office of Electoral Processes of Peru, including the compliance of the e-voting solution with software development, software testing, security and data encryption standards as well as the evaluation of the risks associated with the use of e-voting and recommended control measures to mitigate these risks.

Additionally, Scytl has actively participated in the development of standards for Internet voting in the United States (through the National Institute of Standards and Technology, the U.S. Electoral Commission, and the Institute of Electrical and Electronics Engineers) and Europe (through the Council of Europe and OASIS). Finally, Scytl's experts have contributed to the IEEE Standards Working Group P-1622 on Voting Systems Electronic for the standardization of EML.